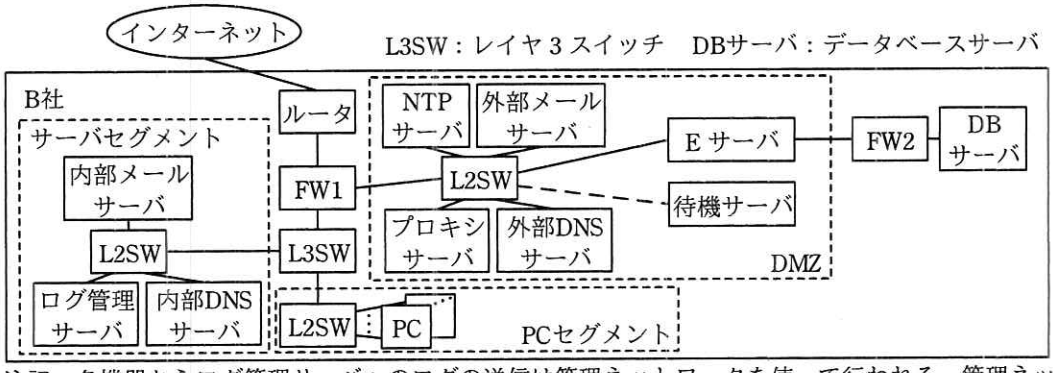
問３　ソフトウェアの脆弱性対策に関する次の記述を読んで，設問 1～5 に答えよ。

B 社は，従業員数 500 名の食品販売会社であり，インターネットを介して消費者向けに食品を通信販売している。

通信販売で使用するシステム（以下，通販システムという）の運用，保守は，B 社の K リーダを中心に，S 君ほか 3 名と協力会社の従業員 5 名の計 10 名で行っている。通販システムを含む B 社情報システムのサーバの概要を表 1 に，構成を図 1 に示す。

表 1　B 社情報システムのサーバの概要（抜粋）

| サーバ名 | 概要 |
|---|---|
| E サーバ | ・通販システムの購入受付処理を行う Web サーバである。また，通販システムのバッチ処理として購入集計処理も行っている。 |
| 待機サーバ | ・E サーバの購入受付処理が停止するなど通販システムの利用者にサービスが提供できなくなった場合に，サービス停止を告知するための Web サーバである。コールドスタンバイしており，E サーバがサービス提供できなくなった場合に E サーバの代わりにレイヤ 2 スイッチ（以下，L2SW という）に接続される。 |
| ログ管理サーバ | ・B 社情報システム中の全ファイアウォール（以下，ファイアウォールを FW という）及び全サーバのログを syslog で受信し保存する。<br>・FW1 及び FW2 のログには，通信の通過や遮断に関する記録がある。<br>・各サーバのログには，OS 上で実行される SSH などのコマンド履歴，アプリケーションやミドルウェアのイベント記録がある。<br>・Web サーバ及びプロキシサーバのログには，送信元及び宛先の IP アドレス，HTTP リクエストの内容，データ転送量などが含まれている。<br>・ログ保全機能があり，それによって，保存したログが改ざんされていないことを証明できる。 |




注記　各機器からログ管理サーバへのログの送信は管理ネットワークを使って行われる。管理ネットワークの記載は省略している。

図 1　B 社情報システムの構成

通販システムは，E サーバ，待機サーバ，FW2 及び DB サーバから構成される。E サーバの購入受付処理は，インターネットから HTTP over TLS（以下，HTTPS という）でアクセスされる。購入集計処理は，バッチプログラムで実行される。毎日午前 2 時開始の日次，毎週土曜日の午前 3 時開始の週次，毎月 1 日午前 4 時開始の月次のバッチプログラムがあり，それぞれ 1 時間以内で処理が完了する。

ログ管理サーバに保存されたログからイベントの発生順序を正しく追跡できるように，①ログに書かれる各 FW 及び各サーバの時刻を整合させている。

FW1 はステートフルパケットインスペクション型で，インターネットと通販システム間の通信は，インターネットから E サーバ及び待機サーバへの HTTPS アクセスとその応答が許可されている。そのほかのインターネットと DMZ 内のサーバ間の通信は，各サーバのサービスに必要なものだけ許可している。

プロキシサーバが中継するのは PC セグメントからインターネットへの通信だけである。

〔脆弱性情報の公開と対応〕

ある日，S 君は，アプリケーションフレームワーク（以下，AF という）のうち，E サーバで使用しているもの（以下，E-AF という）の脆弱性（以下，脆弱性 T という）の情報が，前日に公開されていることを発見し，K リーダに報告した。脆弱性 T の情報を図 2 に示す。

| |
|---|
| ・悪用されるとリモートから任意の OS コマンドを実行されるおそれがある。具体的には，リモートから HTTP リクエストの Content-Type ヘッダフィールドに攻撃コードが挿入されることによって任意の OS コマンドを実行される。<br>・既に攻撃コードやリモート操作用のツールが流通しており，［ a ］[1]による深刻度が高い。 |

注[1] ［ a ］は，基本評価基準，現状評価基準，環境評価基準の三つの基準で脆弱性の深刻さを評価するシステムである。

図 2　脆弱性 T の情報（概要）

脆弱性 T の情報が公開されると同時に，E-AF の脆弱性修正プログラム（以下，パッチという）が公開されていたが，K リーダは，パッチを適用するには，通販システムの動作に影響がないことの確認が必要な上，もし何らかの影響がある場合，通販

システムを修正するなど時間が掛かることになり，営業上大きな機会損失となることを懸念した。K リーダは，パッチを適用するために通販システムを直ちに停止させるよりも，当面は稼働を継続させつつ，半月後の定期メンテナンス作業時に，影響の確認と必要な修正をできるだけ短時間に実施する方が望ましいと考えた。

〔セキュリティインシデントの発生と対処〕

脆弱性 T の情報を S 君が発見してから 2 日後，E サーバの日次バッチ処理が異常終了するという事象が発生した。S 君が確認したところ，日次バッチプログラムの内容が，見覚えのないスクリプト（以下，スクリプト U という）に書き換えられていた。スクリプト U は，B 社と関係のないサイト Z からプログラムをダウンロードして起動したり，コマンド履歴を参照したりするなどの内容であった。

S 君は，スクリプト U を外部記憶媒体に証拠保全した後，日次バッチプログラムをリカバリした。リカバリ後，日次バッチプログラムを実行し，正常に処理されたことを確認した。さらに，E サーバのほかのバッチプログラムを調査して，改ざんされていないことを確認し，K リーダに状況を報告した。

K リーダは，顧客データが大量に漏えいするなどの重大なセキュリティインシデント（以下，セキュリティインシデントをインシデントという）の可能性もあると考え，専門家による調査を緊急に行うことを経営陣に提案した。K リーダは経営陣の承認を得て，②被害拡大を防止するために必要な措置を S 君に指示するとともに，セキュリティ専門会社にインシデントの調査を依頼した。

〔インシデントの調査〕

依頼を受けたセキュリティ専門会社は，インシデントを調査し，3 日後に調査結果を B 社に報告した。セキュリティ専門会社による調査結果を図 3 に示す。

調査によって，次が判明した。
(1) 脆弱性Tを悪用した攻撃の痕跡が見つかった。
(2) スクリプトUは，次の二つを並列で実行するものであったことから，今回の攻撃の主たる目的は，仮想通貨採掘用プログラム（以下，AP1という）を実行することであったと考えられる。
  a) AP1，及びAP1を動作させるのに必要な複数のライブラリをサイトZからHTTPを使ってダウンロードし，AP1を実行する。
  b) コマンド履歴から，SSHコマンドの接続先IPアドレスを全て抽出する。IPアドレスが抽出された場合は，IPアドレスで示される各機器に対し，SSHコマンドで接続を試行し，成功するとその機器上でスクリプトUを実行する。IPアドレスが抽出されなかった場合は，何もしない。
(3) FW1のログを調査した結果，上記(2)a)でのダウンロードは，FW1でブロックされていた。また，B社情報システムのどの機器にもAP1は見つからなかった。
(4) ③Eサーバのコマンド履歴には，SSHコマンドの接続先IPアドレスが含まれておらず，スクリプトUによるほかの機器への接続はなかったと考えられる。このことを確認するために，ほかの機器へのアクセス記録を調査したところ不審なものはなかった。
(5) 顧客データが大量に漏えいした可能性は低い。

図3　セキュリティ専門会社による調査結果（抜粋）

重大な被害は認められなかったものの，脆弱性Tが悪用されて改ざんが行われていたことが明らかになったことから，パッチを適用することにした。パッチを適用し，サービスを再稼働できたのは，インシデント発生から10日後だった。

〔リスク軽減策の検討〕

セキュリティ専門会社からは，脆弱性情報が公開されると，その後間もなく攻撃が急増することが多いことから，脆弱性情報が公開された際に迅速に対応できるようにあらかじめ対応を検討しておくべきであるとアドバイスを受けた。そこで，今回のインシデントも踏まえて，KリーダとS君はAFなどを利用しているシステムの脆弱性が公開された際の対応について検討した。次は，このときのS君とKリーダの会話である。

S君　：AFの脆弱性情報が公開された際は，早期に対応することが望まれます。その点では，暫定的な対策としてWAFの導入が有効との話をよく聞くので，調査しました。

Kリーダ：どうだったかな。

S君　：脆弱性Tについては，情報が公開されてから1日以内にシグネチャが提供されたWAFがありました。

Kリーダ　：通販システムではパッチの適用作業に 7 日掛かったが，それより，WAF による対応の方が早かったようだな。しかし，WAF による対応では，通販システムへの影響があるのではないか。

S君　　：影響があるので，導入時には遮断はせずにアラートを通知するだけのモニタリングモードを用いて検証します。ただし，このモードでは，アラートが通知された際に検知した通信が［　b　］であるかどうかを直ちに確認しなければなりません。もし，［　b　］であった場合は，場合によっては E サーバの停止が必要となります。また，［　b　］ではなかった場合は，WAF のシグネチャの見直しが必要となります。これら一連の手順を決めておかなければなりません。

Kリーダ　：分かった。次に，WAF の選定方法について，確認しておこう。

S君　　：WAF には，大きく分けると，ソフトウェア型，ハードウェア型，クラウド型の 3 種類があります。いずれもモニタリングモードを実現する機能と攻撃とみなされる通信を遮断する機能があります。さらに，④暗号通信に関する機能が用意されているものがあります。

Kリーダ　：なるほど。導入はどのようにするのかな。

S君　　：ソフトウェア型 WAF の場合は，E サーバに導入します。ハードウェア型 WAF の場合は，図 1 中の DMZ 内の L2SW と E サーバとの間に設置します。クラウド型 WAF の場合は，サービス事業者がインターネット上で運用しているものを利用します。クラウド型 WAF を利用する場合は，幾つか設定変更が必要です。例えば，図 1 中の［　c　］の設定を変更して，E サーバへのアクセス経路をクラウド型 WAF 経由に変える必要があります。クラウド型 WAF の IP アドレスが変更された場合でも［　c　］の設定に影響が出ないように，［　d　］レコードを定義して，そのレコードに E サーバの別名としてクラウド型 WAF サービスの事業者が指定する FQDN を記述することが推奨されています。

Kリーダ　：なるほど。当社にはどの種類が適しているか調査してくれ。

S君　　：分かりました。

調査の後，B 社では，WAF を選定し，導入した。以降，攻撃を数多く受けたが，WAF が遮断し，E サーバへの侵入は起きていない。

設問 1　本文中の下線①を実現するための手段を 15 字以内で述べよ。

設問 2　図 2 中の [ a ] に入れる適切な字句を英字 4 字で答えよ。

設問 3　本文中の下線②について，K リーダが S 君に指示した措置を，30 字以内で述べよ。

設問 4　図 3 中の下線③について，コマンド履歴に SSH コマンドの接続先 IP アドレスが含まれていた場合，スクリプト U の内容を考慮すると更に調査が必要となる。仮に接続先 IP アドレスとして外部メールサーバが履歴に含まれていた場合，どの機器のログで，何を調査すべきか。調査すべき機器の名称を図 1 中から選び答えよ。また，調査すべき内容を 30 字以内で，具体的に述べよ。

設問 5　〔リスク軽減策の検討〕について，(1) ～(3) に答えよ。

(1)　本文中の [ b ] に入れる適切な字句を 5 字以内で答えよ。

(2)　B 社で，ハードウェア型 WAF を導入する場合，通販システム利用者の通信プロトコルを考慮すると本文中の下線④の機能が必要である。その機能を 30 字以内で具体的に述べよ。

(3)　本文中の [ c ] に入れる適切なサーバ名を図 1 中から選び答えよ。また，本文中の [ d ] に入れる適切なレコードの名称を答えよ。